Amendments to the Drawings

In the attached replacement drawing sheet, Fig. 8, reference numeral 530b is changed to 830b, and reference numeral 532 is changed to 832.

REMARKS

1. The undersigned thanks the examiner Mr. Hadi Armouche and his supervisor Mr. Gilberto Barron for a very helpful interview conducted February 23, 2009. The interview summary is provided below.

2. The ***specification*** was objected to because it includes hyperlinks, considered to be browser-executable code. The specification is amended herein to insert dashes into the hyperlinks, and more particularly to replace "http" with "h-t-t-p", thereby precluding a computer browser from interpreting the hyperlinks as executable code. At the interview, the examiners suggested inserting underscores, but the underscores merge with underlining required for the inserted text.

3. The abstract is amended to delete expressions objected to by the office action paragraph 6.

4. In the drawings, Fig. 8 was objected to. Fig. 8 is amended herein as suggested by the office action.

5. The claims were objected to due to an error in claim numbering. The claims are renumbered by this amendment.

6. The office action paragraph 12 rejects claims 156-183 under 35 U.S.C. 112, first paragraph (written description requirement) due to lack of description, in the application as filed, of "a manufacture comprising a computer-readable computer program ...". As agreed at the interview, the description is in fact provided in the original application at paragraph 192 referring to a memory (which is a manufacture) and to "program code".

7. The office action paragraph 14 rejects claims 2-17, 19-26, 117-183 and claims 1 and 18 under 35 U.S.C. 112, second paragraph as indefinite for reciting "the method comprising one or more operations". In response, such recitations are deleted from the independent claims 1 and 18, and further:

- Independent claim 1 is spit into three independent claims 1, 184, 203 (which are discussed in more detail below in connection with the section 102 rejection). Some of the

claims dependent from claim 1 are replicated, i.e. corresponding claims are added to depend from claims 184 and 203.

- Independent claim 18 is split into three independent claims 18, 218, 229; some of the dependent claims are replicated.

It was agreed at the interview that splitting claim 1 into three independent claims such as presented herein would overcome the rejection.

8. The office action paragraph 15 rejects claims 156-183 under 35 U.S.C. 112, second paragraph as indefinite for reciting "a manufacture". The office action states that it is unclear what the term "manufacture" encompasses.

As described at the interview, the term "manufacture" has the same meaning as in 35 U.S.C. 101 ("Whoever invents or discovers any new and useful process, machine, **manufacture**, or composition of matter ..., may obtain a patent therefor ..."). It was agreed at the interview that "manufacture" reads on "memory" in the specification paragraph 192, and the term "manufacture", while not limited to the memory, includes a computer readable medium and is clear.

9. Paragraph 16 rejects claims 1 and 18 under 35 U.S.C. 112, second paragraph, for lack of antecedent basis. It was agreed at the interview that the rejection would be withdrawn if claim 1 was amended as presented herein.

Claim 18 is similarly amended.

10. Claims 1-26, 117-183 were rejected under 35 U.S.C. 101 due to claimed processes not being tied to a particular machine and not transforming the underlying subject matter as required by the Federal Circuit decision *In re Bilski et al.*, 88 USPQ 2d 1385 (2008). Independent claims 1, 18, 184, 203, 218, 229 now recite a machine. It was agreed at the interview that a machine recitation in claim 1 would overcome the rejection.

It is noted also that claims 156-183 are not process claims.

11. Claims 156-183 were rejected under 35 U.S.C. 101 for reciting non-statutory subject matter. These claims recite a manufacture, and are amended to recite a "computer-readable manufacture". It was agreed at the interview that "manufacture" was a statutory

subject matter. See *In re Nuijten*, 500 F.3d 1346, 1356-1357; 84 U.S.P.Q.2d 1495 (Fed.Cir. 2007), ruling that a claim to a "signal with embedded … data" is invalid under 35 U.S.C. 101 because, among other things, a signal is not a manufacture (which is a statutory category).

12. Claims 1 and 18 were rejected under 35 U.S.C. 102(e) over U.S. patent no. 7,113,594 to Boneh et al.

12A. Before providing a formal analysis of the Boneh reference, an informal discussion of some aspects of some embodiments the present invention will now be provided for the purposes of. This discussion is not limiting.

In public key/private key encryption, a sender encrypts a message using the recipient's public key. The recipient decrypts the message using his private key. The public and private keys can be generated by the recipient so that no one knows the secret key except for the recipient (i.e. there is no "key escrow"). This is important. As explained below, in the system described in Boneh's column 15 ("BasicIndent"), the secret key $d_{ID}=sQ_{ID}$ is generated by a third party called PKG (private key generator), and hence is known to the PKG in addition to the recipient. Key escrow creates a security risk as explained in the applicant's specification paragraph 14.

As stated above, in some cryptosystems, the public and private keys can be generated by the recipient, and hence there is no key escrow. However, there is another risk: an imposter may send his own public key to the sender in an email purporting to be from the recipient and representing the imposter's public key as being the recipient's public key. The sender will encrypt messages with the imposter's public key, and these messages can be decrypted by the imposter. This problem will be called a "faked-public-key problem" herein. To deal with this problem, the sender must make sure that the public key belongs to the recipient. This assurance can be provided by a trusted third party called "Certification Authority" (CA), who may issue a digital certificate including the recipient's public key and certifying that the public key belongs to the recipient (e.g. identifying the recipient by name or email address; see the applicant's specification paragraph 6). The certificate is signed with the CA's secret key, and the sender can verify the signature with the CA's public key

(this public key cannot be replaced by the imposter because the public key may be well known, e.g. incorporated into standard software).

However, the certificates create a problem of certificate revocation. If the imposter steals the recipient's secret key, then the recipient's public key must not be used, i.e. the certificate must be revoked. The potential senders must be notified of the certificate revocation. Notifying the potential senders can be difficult as explained in the specification paragraphs 7-11.

Boneh offers a different solution to the faked-public-key problem. Boneh's solution does not need certificates. This is because Boneh uses identity-based-encryption, i.e. the recipient's public key itself identifies the recipient. For example, the public key ("ID" in Boneh's column 15 lines 41-43) may include the recipient's name, or email address, or telephone number, or a combination of parameters identifying the recipient. See Boneh's column 2 lines 1-15; column 29 lines 22-33. However, the corresponding secret key must include some secret information and not just the public information "ID". Also, the encryption must be somehow relate to the secret information. In Boneh's column 15, the relationship is provided via a secret "s" of a trusted third party, called PKG (public key generator). This secret "s" is used to generate both the recipient secret key d_{ID} and a public parameter P_{pub} used for encryption. More particularly, $d_{ID}=sQ_{ID}$ where Q_{ID} is a function of ID, and $P_{pub}=sP$. See Boneh's column 15 ("BasicIndent"), Step 2 in line 27; the EXTRACT procedure in lines 40-44; and the encryption in column 15 line 57. Generation of the secret key by the PKG means there is a key escrow as explained above.

Some embodiments of the applicant's invention provide an improved solution to the faked-public-key problem. This solution combines (1) conventional cryptography, with public and private keys generated by the recipient and the private key not available to third parties; and (2) identity-based encryption, with a second set of public and private keys, called encryption and decryption keys to avoid confusion with the keys in (1). The key escrow is eliminated because the private key in (1) is available only to the recipient. Further, there is no need for a certificate because the encryption key in (2) identifies the recipient. The corresponding decryption key may be available to a third party (PKG), but this key is

insufficient to decrypt because decryption requires both the decryption key and the private key. The public key can be faked by an imposter, but the imposter cannot decrypt without the decryption key.

The above informal discussion does not aim at complete description of Boneh or of the present invention. For example, Boneh teaches a Distributed PKG to alleviate the key escrow problem (see Boneh's column 24 line 51 and subsequent text). Also, claims 1 and 18 are not limited to identity-based encryption.

12B. A formal analysis of claim 1 and 18 will now be provided. Claim 1 recites "a key generation secret of the authorizer". The authorizer can be a PKG (specification paragraph 73). The key generation secret reads on s_C in paragraph 77. The claims are not limited to the embodiments discussed herein.

Claim 1 recites:

> encrypting ... the digital message M using ... a recipient public key and a recipient encryption key ... for decryption with a recipient private key and a recipient decryption key, wherein:
>
> the recipient public key and the recipient private key form a public key/ private key pair, wherein the recipient private key is a secret of the recipient;
>
> the recipient decryption key is generated using ... a key generation secret of the authorizer and the recipient encryption key, wherein a key formed from the recipient encryption key and a key formed from the recipient decryption key are a pubic key/ private key pair.

Thus, claim 1 recites two public key/ private key pairs. Assuming for the sake of argument that the applicant's encryption key/ decryption key pair reads on Boneh's ID/d_{ID} pair in column 15 ("BasicIndent"), Boneh does not teach or suggest an additional public key/ private key pair, with the private key being a secret of the recipient as recited in claim 1.

Claim 18 distinguishes over Boneh for similar reasons.

13. If a fee is required for this submission, please charge the fee or any underpayment thereof, or credit any overpayment, to deposit account 50-2257.

Any questions regarding this case can be addressed to the undersigned at the telephone number below.

Certificate of Transmission: I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (USPTO) via the USPTO's electronic filing system on March 4, 2009.

Michael Shenker 3-4-09

Attorney for Applicant(s) Date of Signature

Respectfully submitted,

Michael Shenker

Michael Shenker
Patent Attorney
Reg. No. 34,250
Telephone: (408) 392-9250

Law Offices Of
Haynes and Boone, LLP
2033 Gateway Place, Suite 400
San Jose, CA 95110